



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,932	03/09/2004	Akio Sakamoto	60054-0016	3286

29989 7590 02/28/2007
HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

VAUTROT, DENNIS L

ART UNIT	PAPER NUMBER
----------	--------------

2167

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/796,932

Applicant(s)

SAKAMOTO ET AL.

Examiner

Dennis L. Vautrot

Art Unit

2167

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 November 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>11/22/2006 & 8/28/2006</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements (IDS) submitted on 22 November 2006 and 28 August 2006 have been received and entered into the record. Page 4 of the 22 November 2006 IDS contains duplicate citations to the references on the 28 August 2006 IDS, and therefore were crossed out on the 22 November IDS. Since the IDS comply with the provisions of MPEP § 609, the references cited therein have been considered by the examiner. See attached forms PTO-1449.

Claim Rejections - 35 USC § 101

2. The 101 rejections for claims 15 – 28 have been withdrawn in light of the amendments to the claims.

Response to Amendment

3. The applicants' amendment, filed 27 November 2006, has been received, entered into the record and considered.

4. As a result of the amendment, claims 1, 3 – 5, 8, and 15 – 30 were amended. Claims 1 – 30 are pending in the application.

Response to Arguments

5. Applicant's arguments with respect to claims 1 – 30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1 – 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Examiner believes that there was not proper disclosure in the original application for the amendments received.

Specifically the following language is found to lack support in either the specification or previous version of the claims: "submitting a first set of one or more database queries, to a database server that manages the database, to retrieve, from the database server..."; "...user behavior data that was retrieved from the database server in response to the first set of one or more database queries being executed against the database"; and "submitting a second set of one or more database queries, to the database server, to retrieve, from the database server...". There is also no mention of "a second set of database queries...", as receiving a new set of data, could be performed in a variety of methods not involving queries. There are various ways of collecting user behavior, not involving database queries, and because database queries

Art Unit: 2167

were not mentioned in the specification or initial version of the claims, the amendments appear to be new matter.

These limitations are found in each of the independent claims, and therefore they are all rejected for this reason. However, in order to further prosecution, the claims as amended, including what is considered to be new matter, have been used for this office action, despite the 112 rejection.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1 – 5, 14, 29 and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by **Mattson** (EP 1 315 065 A1).

10. Regarding claim 1, **Mattson** teaches a method for monitoring a database, comprising: submitting a first set of one or more database queries, to a database server that manages the database, to retrieve, from the database server, user behavior data [record] that indicates a first set of one or more actions performed, by one or more

users, as a result of the one or more users executing a first set of database statements against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items."

Although "submitting a first set of one or more database queries" is not explicitly disclosed, it is inherent that if the module is storing results from queries, which creates a record of behavior data, that the queries necessarily must have been submitted to the database server.);

processing and storing one or more sets of user behavior data [accumulated access] as historical data, said one or more sets of user behavior data including said user behavior data that was retrieved from the database server in response to the first set of one or more database queries [results from queries] being executed against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items.");

analyzing the historical data [record] to determine behavior patterns [security policies] (See column 4, paragraphs [0027] and [0028] "If advantageous, the record can be kept in a separate log file 15, for long term storage, accumulating data access over a longer period of time. The server 2 further has access to a plurality of security policies 20, preferably one for each user, one for each defined security role, or the like. These security policies can be stored in the security administration system 8, but also be stored outside the sever. Each policy 20 includes one or several item access rates 21

Art Unit: 2167

and optionally an interference pattern 22." The combined historical access rates and interference patterns are interpreted to be analyzed into the security policies that represent the behavior patterns.);

submitting a second set of one or more database queries [request], to the database server, to retrieve, from the database server, a new set of data that indicates a second set of one or more actions performed by, the one or more users, as a result of the one or more users executing a second set of database statements against the database (See column 5, paragraph [0034] "With reference to fig 2, a request is received by the server in step S1, resulting in the generation of a result in step S2, i.e. a number of selected rows from one or several table columns... If however, marked items are included in the result, the intrusion detection component 13 stores the query result, or at least those parts referring to the marked items, in the record 14, and the program control initiates the intrusion detection.");

performing a comparison between the new set of data [current query result and updated record] and the determined behavior patterns [security policy] (See column 5, paragraph [0035] "... 18 compares the current query result and the updated record 14 with the item access rate 21 included in the security policy associated with the current user, the role that the user belongs to, or the server the user is connected to.");

determining based on the comparison, whether the new set of data satisfies a set of criteria (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion...");

if the new set of data satisfies the set of criteria [...number of rows exceeding...], then determining that the new set of data represents anomalous [intrusion] activity (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion..."); and

responding to the determination by performing a targeted operation (See column 5 paragraph [0036] "...and the access control system 7 will be alerted...").

11. Regarding claim 2, **Mattson** teaches determining if the new set of data [current query result] violates a rule based policy [security policy]; and if the new set of data violates the rule based policy (See column 5, paragraph [0035] "...compares the current query result and the updated record 14 with the item access rate 21 included in the security policy associated with the current user, the role that the user belongs to, or the server the user is connected to."), then determining that the new set of data represents anomalous [intrusion] activity. (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion...")

12. Regarding claim 3, **Mattson** teaches submitting the first set of one or more database queries to the database server further comprises: reading information from an audit trail or dynamic performance views of a database manager. (See column 4, paragraph [0027] "...thereby creating a record 14 of accumulated access of marked

items.” The audit trail description in the instant application's specification in paragraph [0009] refers to information about database accesses, which is what is represented by the quote.)

13. Regarding claim 4, **Mattson** teaches submitting the first set of one or more database queries to the database server further submitting the first set of one or more database queries to the database server at a monitoring level selected from at least one of: information about database access for one or more selected database objects [selected item] (See column 4, paragraph [0029] “...rows of the selected item (e.g. column of a table)...”); information about database access for one or more selected database users (See column 4, paragraph [0029] “...that a given user, role or server...”); and information about database access for one or more selected database user sessions. (See column 4, paragraph [0029] “...during a given period of time.”)

14. Regarding claim 5, **Mattson** teaches submitting the first set of one or more database queries to the database server further comprises: receiving a type of information to be monitored; (See column 4, paragraph [0026] “A first component 12 of the intrusion detection module 10 enables marking of some or all data items in the database, thereby indicating that these items should be monitored during the intrusion detection process...”); determining a monitoring level from the type of information; and activating audit options of the database manager based upon the monitoring level determined. (See column 4, paragraph [0029] “An item access rate 21 defines the

maximum number of rows of the selected item (e.g. column of a table) that a given user, role, or server may access during a given period of time.”) Here, the monitoring level is based on the selected database object, the column of a table, and the audit option is based on the access to that column, as in the claim.)

15. Regarding claim 14, **Mattson** teaches performing a targeted operation comprises at least one of: raising an alert; sending an email; producing a report; performing a visualization. (See column 5, paragraph [0036] “...and the access control system 7 will be alerted.”)

16. Regarding claim 29, **Mattson** teaches an apparatus comprising:

means for submitting a first set of one or more database queries, to a database server that manages the database, to retrieve, from the database server, user behavior data [record] that indicates a first set of one or more actions performed, by one or more users, as a result of the one or more users executing a first set of database statements against the database (See column 4, paragraph [0027] “A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items.” Although “submitting a first set of one or more database queries” is not explicitly disclosed, it is inherent that if the module is storing results from queries, which creates a record of behavior data, that the queries necessarily must have been submitted to the database server.);

means for processing and storing one or more sets of user behavior data [accumulated access] as historical data, said one or more sets of user behavior data including said user behavior data that was retrieved from the database server in response to the first set of one or more database queries [results from queries] being executed against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items.");

means for analyzing the historical data [record] to determine behavior patterns [security policies] (See column 4, paragraphs [0027] and [0028] "If advantageous, the record can be kept in a separate log file 15, for long term storage, accumulating data access over a longer period of time. The server 2 further has access to a plurality of security policies 20, preferably one for each user, one for each defined security role, or the like. These security policies can be stored in the security administration system 8, but also be stored outside the sever. Each policy 20 includes one or several item access rates 21 and optionally an interference pattern 22." The combined historical access rates and interference patterns are interpreted to be analyzed into the security policies that represent the behavior patterns.);

means for submitting a second set of one or more database queries [request], to the database server, to retrieve, from the database server, a new set of data that indicates a second set of one or more actions performed by, the one or more users, as a result of the one or more users executing a second set of database statements

against the database (See column 5, paragraph [0034] "With reference to fig 2, a request is received by the server in step S1, resulting in the generation of a result in step S2, i.e. a number of selected rows from one or several table columns...If however, marked items are included in the result, the intrusion detection component 13 stores the query result, or at least those parts referring to the marked items, in the record 14, and the program control initiates the intrusion detection.");

means for performing a comparison between the new set of data [current query result and updated record] and the determined behavior patterns [security policy] (See column 5, paragraph [0035] "... 18 compares the current query result and the updated record 14 with the item access rate 21 included in the security policy associated with the current user, the role that the user belongs to, or the server the user is connected to.");

means for determining based on the comparison, whether the new set of data satisfies a set of criteria (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion...");

if the new set of data satisfies the set of criteria [...number of rows exceeding...], then determining that the new set of data represents anomalous [intrusion] activity (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion..."); and

means for responding to the determination by performing a targeted operation (See column 5 paragraph [0036] "...and the access control system 7 will be alerted...").

17. Regarding claim 30, **Mattson** teaches an apparatus comprising:

a data collector for (a) collecting user behavior data that indicates a first set of one or more actions performed, by one or more users, as a result of the one or more users executing a first set of database statements against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items." Although "submitting a first set of one or more database queries" is not explicitly disclosed, it is inherent that if the module is storing results from queries, which creates a record of behavior data, that the queries necessarily must have been submitted to the database server.), (b) processing and storing the one or more sets of user behavior data [accumulated access] as historical data, said one or more sets of user behavior data including said user behavior data that was retrieved from the database server in response to the first set of one or more database queries [results from queries] being executed against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items."), and (c) submitting a second set of one or more database queries [request], to the database server, to retrieve, from the database server, a new set of data that indicates a second set of one or more actions performed by, the one or more users, as a result of the one or more users executing a second set of database statements against the database (See column 5, paragraph

Art Unit: 2167

[0034] "With reference to fig 2, a request is received by the server in step S1, resulting in the generation of a result in step S2, i.e. a number of selected rows from one or several table columns...If however, marked items are included in the result, the intrusion detection component 13 stores the query result, or at least those parts referring to the marked items, in the record 14, and the program control initiates the intrusion detection.");

a data analyzer for analyzing the historical data [record] to determine behavior patterns [security policies] (See column 4, paragraphs [0027] and [0028] "If advantageous, the record can be kept in a separate log file 15, for long term storage, accumulating data access over a longer period of time. The server 2 further has access to a plurality of security policies 20, preferably one for each user, one for each defined security role, or the like. These security policies can be stored in the security administration system 8, but also be stored outside the sever. Each policy 20 includes one or several item access rates 21 and optionally an interference pattern 22." The combined historical access rates and interference patterns are interpreted to be analyzed into the security policies that represent the behavior patterns.); and

an anomaly detector for (a) performing a comparison between the new set of data [current query result and updated record] and the determined behavior patterns [security policy] (See column 5, paragraph [0035] "... 18 compares the current query result and the updated record 14 with the item access rate 21 included in the security policy associated with the current user, the role that the user belongs to, or the server the user is connected to."), (b) determining based on the comparison, whether the new

set of data satisfies a set of criteria (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion..."), (c) determining that the new set of data represents anomalous [intrusion] activity (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion..."), and (d) responding to the determination by performing a targeted operation (See column 5 paragraph [0036] "...and the access control system 7 will be alerted...").

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. Claims 6 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mattson** in view of **Sekiguchi** (EP 0 999 490).

20. Regarding claim 6, **Mattson** discloses a method substantially as claimed.

Mattson does not explicitly disclose analyzing the historical data to determine behavior

patterns further comprises: determining a statistical model from the historical data. However **Sekiguchi** teaches analyzing the historical data to determine behavior patterns further comprises: determining a statistical model from the historical data. (See column 6, paragraph [0030] "The security management unit 112 executes the statistical process of the access log 201 which is acquired by the access log acquisition unit 111...") It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include analyzing the historical data to determine behavior patterns further comprises: determining a statistical model from the historical data.

21. Regarding claims 7, **Mattson** discloses a method substantially as claimed. **Mattson** does not explicitly disclose determining a statistical model from the historical data further comprises: determining a frequency of database access from the historical data; determining a probability function for frequencies of database access; and determining a cumulative probability function from the probability function. However, **Sekiguchi** teaches determining a statistical model from the historical data further comprises: determining a frequency of database access from the historical data [access log] (See column 6, paragraph [0030] "...converts the access log to security management information 203, such as the frequency of access..."); determining a probability function [statistical process] for frequencies of database access (See column

7, paragraph [0035] "For this reason, the security management unit 112 manages information about a time zone using a method for determining the scope of the time zone where access is gained with a statistical process."); and determining a cumulative probability function from the probability function (See column 7, paragraph [0035] "Such statistical information about an access is calculated for all accesses without dividing a section or by dividing a section of, for example, the past one month or one year, if necessary, and the time zone in which an access is permitted is set based on the calculation." The function or process referred to is clearly cumulative based on the discussion of the statistical process (or probability function).)

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include determining a statistical model from the historical data further comprises: determining a frequency of database access from the historical data; determining a probability function for frequencies of database access; and determining a cumulative probability function from the probability function.

22. Regarding claim 8, **Mattson** discloses a method substantially as claimed. **Mattson** does not explicitly disclose performing a comparison between the new set of data and the determined behavior patterns further comprises: testing a hypothesis using the new set of data against the statistical model. However, **Sekiguchi** teaches

performing a comparison between the new set of data [access log] and the determined behavior patterns [security management information] further comprises: testing a hypothesis using the new set of data [access log] against the statistical model [process] (See column 6, paragraph [0030] "The security management unit 112 executes the statistical process of the access log 201 which is acquired by the access log acquisition unit 111, converts the access log to security management information 203....").

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include performing a comparison between the new set of data and the determined behavior patterns further comprises: testing a hypothesis using the new set of data against the statistical model.

23. Regarding claim 9, **Mattson** discloses a method substantially as claimed. **Mattson** does not explicitly disclose testing a hypothesis using the new set of data against the statistical model further comprises: determining a frequency of database access for the new set of data. However, **Sekiguchi** teaches testing a hypothesis using the new set of data against the statistical model further comprises: determining a frequency of database access for the new set of data [access log] (See column 6, paragraph [0030] "converts the access log to security management information, such as the frequency of access to the file..."); and determining the threshold value [scope of the time zone] from a guard criteria [plus/minus 3s] and a probability function parameter

Art Unit: 2167

[statistical process] (See column 7, paragraph [0035] "For this reason, the security management unit 112 manages information about a time zone using a method for determining the scope of the time zone where access is gained with a statistical process...a time zone from which a user access is judged to be normal is assumed to be a scope of plus/minus 3s... If this method is adopted, the access time zone of a user automatically changes according to the use situation of the user, regardless of its initial setting, thus making it convenient.")

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include testing a hypothesis using the new set of data against the statistical model further comprises: determining a frequency of database access for the new set of data.

24. Regarding claim 10, **Mattson** discloses a method substantially as claimed. **Mattson** does not explicitly disclose testing a hypothesis using the new set of data against the statistical model pattern further comprises: comparing the frequency of database access for the new set of data with the threshold value. However, **Sekiguchi** teaches testing a hypothesis using the new set of data [access log] against the statistical model pattern [security management information] further comprises: comparing the frequency of database access [included in the access log] for the new set of data [access log] with the threshold value [access situation] (See column 7,

Art Unit: 2167

paragraph [0036] "A log comparison unit 115 compares the access log 201 of this time which is acquired by the access acquisition unit 111 with the access situation of security management information 203 which is acquired from log information acquired before.")

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include testing a hypothesis using the new set of data against the statistical model pattern further comprises: comparing the frequency of database access for the new set of data with the threshold value.

25. Regarding claim 11, **Mattson** discloses a method substantially as claimed.

Mattson does not explicitly disclose the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location. However, **Sekiguchi** teaches the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data [access log] further

Art Unit: 2167

comprises determining a frequency of at least one of: object access frequency by hour of day [access date and time], object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location. (See column 6, paragraph [0030] "...the access log acquisition unit 111 converts the access log to security management information 203, such as the frequency of access, the time zone of access data and time... the name of a file accessed in the past, the frequency of access to the file... Alternatively, the access log 201 can be statistically processed for each file or computer, and can be stored as security management information 203.")

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location.

Art Unit: 2167

26. Regarding claim 12, **Mattson** discloses a method substantially as claimed.

Mattson does not explicitly disclose the historical information is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: user access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location. However, **Sekiguchi** teaches the historical information [access log] is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: user access frequency by hour of day [access time], user access frequency by hour of day and operating system user [access time and user A], user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location. (See column 8, paragraph [0039] "...if the access log 201 of the user A is as shown in Fig. 3 and the security management information 203 as shown in Fig 4 is stored for the user A, the access time is 18:30:34...In this case the access is judged to be normal and it is checked whether the access violates the access restriction.")

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the

Art Unit: 2167

determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include the historical information is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: user access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location.

27. Regarding claim 13, **Mattson** teaches a method substantially as claimed.

Mattson does not explicitly disclose the historical information is about database access for one or more selected database user sessions and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: number of page reads per session, access duration per session, number of page reads per unit time. However, **Sekiguchi** teaches the historical information is about database access for one or more selected database user sessions [access situation] and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: number of page reads per session [frequency of access], access duration per session [elapsed time], number of page reads per unit time [frequency of access]. (See **Sekiguchi** column 3, paragraph [0016] "modifying a setting file to be used according to the access

situation of a user, such as elapsed time, the frequency of accesses etc., and modifying and managing a security level, can be provided in order to manage the security level.”)

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include the historical information is about database access for one or more selected database user sessions and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: number of page reads per session, access duration per session, number of page reads per unit time.

28. Claims 15 – 19 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mattson** in view of **Ho** (6,597,777).

29. Regarding claim 15, **Mattson** teaches a computer readable storage medium carrying one or more sequence of instructions, which instructions, when executed by one or more of the processors, case the one or more processors to carry out the steps of:

submitting a first set of one or more database queries, to a database server that manages the database, to retrieve, from the database server, user behavior data [record] that indicates a first set of one or more actions performed, by one or more users, as a result of the one or more users executing a first set of database statements

against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items."

Although "submitting a first set" is not explicitly disclosed, it is interpreted that if the module is storing results from queries, which creates a record of behavior data, that the queries necessarily must have been submitted to the database server.);

processing and storing one or more sets of user behavior data [accumulated access] as historical data, said one or more sets of user behavior data including said user behavior data that was retrieved from the database server in response to the first set of one or more database queries [results from queries] being executed against the database (See column 4, paragraph [0027] "A second component 13 of the intrusion detection module 10 is adapted to store all results from queries including marked items, thereby creating a record 14 of accumulated access of marked items."));

analyzing the historical data [record] to determine behavior patterns [security policies] (See column 4, paragraphs [0027] and [0028] "If advantageous, the record can be kept in a separate log file 15, for long term storage, accumulating data access over a longer period of time. The server 2 further has access to a plurality of security policies 20, preferably one for each user, one for each defined security role, or the like. These security policies can be stored in the security administration system 8, but also be stored outside the sever. Each policy 20 includes one or several item access rates 21 and optionally an interference pattern 22." The combined historical access rates and

interference patterns are interpreted to be analyzed into the security policies that represent the behavior patterns.);

submitting a second set of one or more database queries [request], to the database server, to retrieve, from the database server, a new set of data that indicates a second set of one or more actions performed by, the one or more users, as a result of the one or more users executing a second set of database statements against the database (See column 5, paragraph [0034] "With reference to fig 2, a request is received by the server in step S1, resulting in the generation of a result in step S2, i.e. a number of selected rows from one or several table columns... If however, marked items are included in the result, the intrusion detection component 13 stores the query result, or at least those parts referring to the marked items, in the record 14, and the program control initiates the intrusion detection.");

performing a comparison between the new set of data [current query result and updated record] and the determined behavior patterns [security policy] (See column 5, paragraph [0035] "... 18 compares the current query result and the updated record 14 with the item access rate 21 included in the security policy associated with the current user, the role that the user belongs to, or the server the user is connected to.");

determining based on the comparison, whether the new set of data satisfies a set of criteria (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion...");

if the new set of data satisfies the set of criteria [...number of rows exceeding...], then determining that the new set of data represents anomalous [intrusion] activity (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion..."); and

responding to the determination by performing a targeted operation (See column 5 paragraph [0036] "...and the access control system 7 will be alerted...").

Mattson does not explicitly disclose reverting to a recovery configuration in response to device faults. However, **Ho** teaches reverting to a recovery configuration [corrective module] in response to device faults [server failure]. (See column 11, lines 7-8 "Upon the onset of a server failure, the failing service class unfairly ties up network resources", lines 12-16 "The present invention, however, detects the fact that the traffic intensity persistently exceeds the upper threshold within the first 15 minutes of the onset of the server failure and detects the service class with which the failure is associated..." lines 26-32 "...one or more corrective control modules connecting detector 604 and network 601, may be responsive to a generated alarm for automatic corrective action...") It would have been obvious to one with ordinary skill in the art at the time of the invention to combine the teachings of **Mattson** with that of **Ho** because they both deal with detecting anomalous activity on electronic systems, and by including a way to handle device faults, the medium becomes more robust than before, allowing faults to not disrupt the monitoring. It is for this reason that one of ordinary skill in the art would

have been motivated to include revering to a recovery configuration in response to device faults.

30. Regarding claim 16, **Mattson** additionally teaches determining if the new set of data [current query result] violates a rule based policy [security policy]; and if the new set of data violates the rule based policy (See column 5, paragraph [0035] "...compares the current query result and the updated record 14 with the item access rate 21 included in the security policy associated with the current user, the role that the user belongs to, or the server the user is connected to."), then determining that the new set of data represents anomalous [intrusion] activity. (See column 5 paragraph [0036] "If the current query result or accumulated record 14 includes a number of rows exceeding a particular item access rate 21, such a result will be classified as an intrusion...")

31. Regarding claim 17, **Mattson** additionally teaches submitting the first set of one or more database queries to the database server further comprises instructions for carrying out the step of: reading information from an audit trail of the database manager. (See column 4, paragraph [0027] "...thereby creating a record 14 of accumulated access of marked items." The audit trail description in the instant application's specification in paragraph [0009] refers to information about database accesses, which is what is represented by the quote.)

32. Regarding claim 18, **Mattson** additionally teaches submitting the first set of one or more database queries to the database server further submitting the first set of one or more database queries to the database server at a monitoring level selected from at least one of: information about database access for one or more selected database objects [selected item] (See column 4, paragraph [0029] "...rows of the selected item (e.g. column of a table)..."); information about database access for one or more selected database users (See column 4, paragraph [0029] "...that a given user, role or server...") and information about database access for one or more selected database user sessions. (See column 4, paragraph [0029] "...during a given period of time.")

33. Regarding claim 19, **Mattson** additionally teaches submitting the first set of one or more database queries to the database server further comprises: receiving a type of information to be monitored; (See column 4, paragraph [0026] "A first component 12 of the intrusion detection module 10 enables marking of some or all data items in the database, thereby indicating that these items should be monitored during the intrusion detection process..."); determining a monitoring level from the type of information; and activating audit options of the database manager based upon the monitoring level determined. (See column 4, paragraph [0029] "An item access rate 21 defines the maximum number of rows of the selected item (e.g. column of a table) that a given user, role, or server may access during a given period of time.") Here, the monitoring level is based on the selected database object, the column of a table, and the audit option is based on the access to that column, as in the claim.)

34. Regarding claim 28, **Mattson** additionally teaches performing a targeted operation comprises at least one of: raising an alert; sending an email; producing a report; performing a visualization. (See column 5, paragraph [0036] "...and the access control system 7 will be alerted.")

35. Claims 20 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mattson** in view of **Ho** as applied to claim 16 above, and further in view of **Sekiguchi**.

36. Regarding claim 20, **Mattson** and **Ho** teach a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose analyzing the historical data to determine behavior patterns further comprise instructions for carrying out the step of: determining a statistical model from the historical data. However, **Sekiguchi** teaches analyzing the historical data to determine behavior patterns further comprise instructions for carrying out the step of: determining a statistical model from the historical data. (See column 6, paragraph [0030] "The security management unit 112 executes the statistical process of the access log 201 which is acquired by the access log acquisition unit 111...") It would have be obvious to one with ordinary skill in the art at the time the invention was made to combine the references because they are related to security monitoring of electronic systems and by including the statistical model teaching as disclosed in **Sekiguchi**, determination can be made more easily for the detection of anomalous activity. It is for this reason that one of

ordinary skill in the art would have been motivated to include analyzing the historical data to determine behavior patterns further comprises: determining a statistical model from the historical data.

37. Regarding claim 21, **Mattson** and **Ho** teach a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose the instructions for carrying out the step of determining a statistical model from the historical data further comprise instructions for carrying out the step of: determining a frequency of database access from the historical data; determining a probability function for frequencies of database access; and determining a cumulative probability function from the probability function. However, **Sekiguchi** teaches the instructions for carrying out the step of determining a statistical model from the historical data further comprise instructions for carrying out the step of: determining a frequency of database access from the historical data [access log] (See column 6, paragraph [0030] "...converts the access log to security management information 203, such as the frequency of access..."); determining a probability function [statistical process] for frequencies of database access (See column 7, paragraph [0035] "For this reason, the security management unit 112 manages information about a time zone using a method for determining the scope of the time zone where access is gained with a statistical process."); and determining a cumulative probability function from the probability function (See column 7, paragraph [0035] "Such statistical information about an access is calculated for all accesses without dividing a section or by dividing a section of, for

Art Unit: 2167

example, the past one month or one year, if necessary, and the time zone in which an access is permitted is set based on the calculation.” The function or process referred to is clearly cumulative based on the discussion of the statistical process (or probability function).)

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** and **Ho** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include determining a statistical model from the historical data further comprises: determining a frequency of database access from the historical data; determining a probability function for frequencies of database access; and determining a cumulative probability function from the probability function.

38. Regarding claim 22, **Mattson** and **Ho** disclose a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose performing a comparison between the new set of data and the determined behavior patterns further comprises: testing a hypothesis using the new set of data against the statistical model. However, **Sekiguchi** teaches performing a comparison between the new set of data [access log] and the determined behavior patterns [security management information] further comprises: testing a hypothesis using the new set of data [access log] against the statistical model [process] (See column 6, paragraph [0030] “The security management unit 112 executes the statistical process of the access log 201 which is

acquired by the access log acquisition unit 111, converts the access log to security management information 203....”).

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** and **Ho** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include performing a comparison between the new set of data and the determined behavior patterns further comprises: testing a hypothesis using the new set of data against the statistical model.

39. Regarding claim 23, **Mattson** and **Ho** disclose a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose testing a hypothesis using the new set of data against the statistical model further comprises: determining a frequency of database access for the new set of data. However, **Sekiguchi** teaches testing a hypothesis using the new set of data against the statistical model further comprises: determining a frequency of database access for the new set of data [access log] (See column 6, paragraph [0030] “converts the access log to security management information, such as the frequency of access to the file...”); and determining the threshold value [scope of the time zone] from a guard criteria [plus/minus 3s] and a probability function parameter [statistical process] (See column 7, paragraph [0035] “For this reason, the security management unit 112 manages information about a time zone using a method for determining the scope of the time zone where access is gained with a statistical process...a time zone from which a user

Art Unit: 2167

access is judged to be normal is assumed to be a scope of plus/minus 3s... If this method is adopted, the access time zone of a user automatically changes according to the use situation of the user, regardless of its initial setting, thus making it convenient.”)

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** and **Ho** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include testing a hypothesis using the new set of data against the statistical model further comprises: determining a frequency of database access for the new set of data.

40. Regarding claim 24, **Mattson** and **Ho** disclose a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose testing a hypothesis using the new set of data against the statistical model pattern further comprises: comparing the frequency of database access for the new set of data with the threshold value. However, **Sekiguchi** teaches testing a hypothesis using the new set of data [access log] against the statistical model pattern [security management information] further comprises: comparing the frequency of database access [included in the access log] for the new set of data [access log] with the threshold value [access situation] (See column 7, paragraph [0036] “A log comparison unit 115 compares the access log 201 of this time which is acquired by the access acquisition unit 111 with the access situation of security management information 203 which is acquired from log information acquired before.”)

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** and **Ho** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include testing a hypothesis using the new set of data against the statistical model pattern further comprises: comparing the frequency of database access for the new set of data with the threshold value.

41. Regarding claim 25, **Mattson** and **Ho** disclose a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location. However, **Sekiguchi** teaches the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data [access log] further comprises determining a frequency of at least one of: object access frequency by hour of day [access date and time], object access frequency by hour of day and operating system user, object access

Art Unit: 2167

frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location. (See column 6, paragraph [0030] "...the access log acquisition unit 111 converts the access log to security management information 203, such as the frequency of access, the time zone of access data and time... the name of a file accessed in the past, the frequency of access to the file...Alternatively, the access log 201 can be statistically processed for each file or computer, and can be stored as security management information 203.")

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** and **Ho** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location.

42. Regarding claim 26, **Mattson** and **Ho** disclose a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose the

Art Unit: 2167

historical information is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: user access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location. However, **Sekiguchi** teaches the historical information [access log] is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: user access frequency by hour of day [access time], user access frequency by hour of day and operating system user [access time and user A], user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location. (See column 8, paragraph [0039] "...if the access log 201 of the user A is as shown in Fig. 3 and the security management information 203 as shown in Fig 4 is stored for the user A, the access time is 18:30:34...In this case the access is judged to be normal and it is checked whether the access violates the access restriction.")

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** and **Ho** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason

that one of ordinary skill in the art would have been motivated to include the historical information is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: user access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location.

43. Regarding claim 27, **Mattson** and **Ho** teaches a computer readable storage medium substantially as claimed. **Mattson** and **Ho** do not explicitly disclose the historical information is about database access for one or more selected database user sessions and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: number of page reads per session, access duration per session, number of page reads per unit time.

However, **Sekiguchi** teaches the historical information is about database access for one or more selected database user sessions [access situation] and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: number of page reads per session [frequency of access], access duration per session [elapsed time], number of page reads per unit time [frequency of access]. (See column 3, paragraph [0016] "modifying a setting file to be used according to the access situation of a user, such as elapsed time,

the frequency of accesses etc., and modifying and managing a security level, can be provided in order to manage the security level.”)

It would have be obvious to one with ordinary skill in the art at the time the invention was made to modify **Mattson** with **Sekiguchi** in order to make the determination more easily for the detection of anomalous activity. It is for this reason that one of ordinary skill in the art would have been motivated to include the historical information is about database access for one or more selected database user sessions and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of: number of page reads per session, access duration per session, number of page reads per unit time.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2167


the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dennis L. Vautrot whose telephone number is 571-272-2184. The examiner can normally be reached on Monday-Friday 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Dv
16 February 2007



JOHN COTTINGHAM
SUPERVISORY PATENT EXAMINER
571-272-7079